WatchGuard System Manager and Fireware™

Release Notes for WSM v10.2.7 and Fireware v10.2.7

Introduction

WatchGuard is pleased to release WatchGuard System Manager (WSM) v10.2.7 management software and Fireware / Fireware Pro v10.2.7 appliance software.

The v10.2.7 release contains a number of defect fixes for issues reported by WatchGuard customers. Areas affected include High Availability, Mobile VPN with SSL, and more. This release also includes the ability to configure QoS and policy schedules for managed branch office VPN tunnels.

See the Resolved Issues section below for a complete list of resolved issues.

Before You Start

Before you install this release, make sure that you have:

- (IMPORTANT) Fireware or Fireware Pro v8.3 or later installed on your Firebox. If you have an earlier version of Fireware installed on your Firebox, you must upgrade to Fireware v8.3 or later before you install Fireware v10.2.7. See the Known Issues section for more instructions.
- (IMPORTANT) A backup copy of your current Fireware or WFS configuration file. To make a backup of the configuration file, see “Configuration Files” in the *WatchGuard System Manager User Guide*.
- (IMPORTANT) A full backup of the Fireware image or Firebox X WFS image. To make a backup of the image, see “Configuration Files” in the *WatchGuard System Manager User Guide*.
- An appropriate Firebox and the required hardware and software components as shown in “WSM v10.2.7 System Requirements” below.
- Feature key for your Firebox – If you are a new user, download this from the WatchGuard LiveSecurity site after you register your Firebox. If you have already registered a Firebox X Core or Peak e-Series and have not updated your feature key since v9.0 was released, download and save a new feature key for your Firebox to take advantage of changes in firewall throughput limits in the feature key.
- Documentation for this product is available at www.watchguard.com/help/documentation

WatchGuard System Manager v10.2.7 Minimum System Requirements

	If you have WatchGuard System Manager client software only installed	If you install WatchGuard System Manager and WatchGuard Server software
Operating System	Windows Vista (32-bit), XP SP2 (32-bit), Windows Server 2003 (32-bit)	Windows Vista (32-bit), Windows XP SP2 (32-bit), Windows Server 2003 (32-bit)
Browser	IE 6, IE 7, Firefox v2	N/A
CPU	Intel Pentium IV	Intel Pentium IV
Processor Speed	1 GHz	2 GHz
Memory	512 MB	1 GB
Available Disk Space	80 MB	1GB

Downloading Software

To download WSM and Fireware v10.2.7:

1. Go to the LiveSecurity web site's Software Downloads page at http://www.watchguard.com/archive/softwarecenter.asp
2. Log in to the LiveSecurity web site. Then, select the product line you use and look for the WSM and Fireware v10.2.7 software download section.

Installation and Upgrade

Before you install the WatchGuard System Manager software, read the information in the Known Issues section below.

Note The WSM v10.2.7 installer is not a full WSM install. To upgrade to WSM v10.2.7 you must have WSM v10.2 or later installed first. Review the WSM v10.2 release notes for the WSM v10.2 install instructions.

To upgrade to WSM and Fireware v10.2.7 if your Firebox is currently running WSM and Fireware v10.2.x

1. Back up your current Firebox image using **Policy Manager File > Backup**.
2. Close all applications and stop all servers using the WatchGuard toolbar before you start to uninstall WSM.
3. If you use a Management Server, make a backup of your Management Server configuration before you upgrade (right-click the Management Server icon and select **Backup/Restore**).
4. Launch WSM10_2_7.exe and follow the on-screen installation directions. Note: You must have WSM v10.2 or later installed before you run the WSM10_2_7.exe.
5. Launch the fireware10_2_7.exe and follow the on-screen installation directions.

6. To upgrade your Firebox to Fireware v10.2.7, use WSM v10.2.7 to connect to the Firebox. Use Policy Manager to open your Firebox X Peak or Firebox X Core configuration file.
7. From Policy Manager, select **File > Upgrade**. Browse to C:\Program Files\Common Files\WatchGuard\resources\Fireware\10.2
8. Select the `FW1020B207454.wgu` file and click **OK**. Wait for the Firebox to reboot. You see a success message when the upgrade is complete.
9. After the image upgrade finishes, select **File > Save > To Firebox** to save the configuration to the Firebox

To install the Fireware or Fireware Pro software for the first time on a Firebox X Core or Peak e-Series device

Use the instructions in the Quick Start Guide to install the software and do the initial configuration.

To upgrade a Firebox X Core from WFS to Fireware appliance software

Use the instructions in the Migration Guide to install this release. You can find a copy of this document at www.watchguard.com/help/documentation. If you currently use your Firebox as a Management Server, you must first upgrade to WSM/Fireware v8.3. After you migrate to WSM/Fireware v8.3 successfully, you can use the instructions above to complete the upgrade to WSM/Fireware v10.2.7.

- When you upgrade a Firebox X from WFS to Fireware, your current Gateway AntiVirus for E-mail and SpamScreen subscriptions stop. This is because these subscriptions only apply to a Firebox X running WFS.
- If you have a current GAV for E-Mail or SpamScreen subscription that has not yet expired, you can purchase the new Gateway AntiVirus/IPS and spamBlocker service subscriptions at a reduced cost. Contact your reseller for more information.
- All LiveSecurity and WebBlocker subscriptions continue with no change when you upgrade.

To obtain and install the Mobile VPN with IPSec v10.1 client software

Use the instructions in the Mobile VPN with IPSec v10.1 release notes, which are posted on the LiveSecurity web site.

To install the v10.2.7 Mobile VPN with SSL client for Windows

The v10.2.7 Mobile VPN with SSL client is integrated into the Fireware 10.2.7 appliance software. Mobile VPN with SSL users can choose to download the v10.2.7 client from the Firebox or download the v10.2.7 client from the WatchGuard web site if the remote users do not have access to the Firebox on port 4100.

When a SSL client computer running an earlier version of the client software connects to a Firebox running v10.2.7, the user sees a prompt to upgrade the SSL client version to 1.13. Select **Yes** to upgrade the Mobile VPN client version to v10.2.6. Mobile VPN with SSL continues to operate if the user chooses not to upgrade, however, the user does not receive the fixes available in the v10.2.7 Mobile VPN with SSL client.

To install Single Sign-On (SSO) software

If you are upgrading from a previous SSO implementation, you must first uninstall the existing SSO agent. With the v10.2.4 release, you can install a new SSO client software package to improve the efficiency and accuracy of your Single Sign-On implementation. See the help system for your Firebox for more information about the new SSO implementation.

To install v10.2.4 Single Sign-On agent software

1. Go to http://www.watchguard.com/support and log in with your LiveSecurity user name and passphrase. Follow the link to the Software Downloads page and download the WatchGuard Single Sign-On Agent 10.2.4. Save the WG-Authentication-Gateway.exe file to your hard disk.
2. Install the file on a domain computer with a static IP address and complete the setup wizard. It is a good idea to install the SSO agent software on your domain controller. For more setup instructions see the Single Sign-On (SSO) Implementation Notes section near the end of this document.

To install v10.2.4 Single Sign-On client software

1. Go to http://www.watchguard.com/support and log in with your LiveSecurity user name and passphrase. Follow the link to the Software Downloads page and download the WatchGuard Single Sign-On Agent 10.2.4. Save the WatchGuard-Authentication-Client.msi file to your hard disk.
2. Because the SSO client installer is an MSI file, you can choose to automatically install it on your user's computers when they log on to your domain. You can use Active Directory Group Policy to automatically install software when users log on to your domain. For more information about software installation deployment for Active Directory group policy objects, go to http://www.microsoft.com.

Resolved Issues

General

- This release resolves a kernel crash associated with branch office VPN and Mobile VPN with IPSec traffic through the Firebox X Core or Peak e-Series. [29491]
- The Firebox no longer stops passing traffic when you save a configuration. [27821]
- Policy Manager no longer prevents the entry of host ranges for 1-to-1 NAT on the BOVPN tunnel route settings page. [30010]
- The Server Load Balancing feature in Fireware now correctly detects that a server is not responding and stops sending traffic to that server. [27276]

WatchGuard System Manager (WSM)

- You can now apply QoS and a schedule when you create a VPN firewall; policy template for managed BOVPN tunnels. [10270]
- You should no longer see the error message "*HTTP response code: 500 for URL https://x.x.x.x:4117/cmm/cmd*" when you try to connect to WSM. [29336]

High Availability

- If there is an active Mobile VPN with PPTP tunnel connected to the Firebox during a configuration save, Firebox System Manager no longer shows the HA peer status as "in-transition." [27557]

- WSM and Firebox System Manager connections no longer fail after a configuration save to two Fireboxes configured in an HA configuration. [31990]

Mobile VPN with SSL

- The Windows SSL VPN client no longer fails to install on Windows XP with a Runtime Error message. [31932]
- The Windows SSL VPN client now operates correctly after a computer returns from sleep mode. [31523]

Known Issues and Limitations

These are known issues for WatchGuard System Manager and Fireware v10.2.7. Where available, we include a way to work around the issue.

Upgrading to Fireware v10.2.7 from Fireware v8.2 and earlier

- It is not possible to upgrade directly to Fireware v10.2.7 from Fireware v8.0, v8.1, or v8.2.x. You must upgrade to Fireware v8.3 before you install Fireware v10.2.7.
- If you use Internet Explorer 6, the web-based Quick Setup Wizard can fail to complete the loading of software and initial configuration onto the Firebox because of the way IE6 handles old cache files and scripts.

> **Workaround**
>
> Clear the file cache in your web browser and try again. To clear the cache: from the Internet Explorer toolbar select **Tools > Internet Options > Delete Files**.

Quick Setup Wizard

- The Quick Setup Wizard installed on your management station sets the IP address of the Log Server in the configuration file to the temporary dynamic IP address on the management station during setup (10.0.1.100/24). [13908]

> **Workaround**
>
> Use the WSM-based Quick Setup Wizard only on a computer with a static IP address on which the Log Server is already installed.

Authentication

- The authentication applet does not load when you use an underscore character "_" in the URL path, such as https://xy_wz:4100. [27196]

> **Workaround**
>
> If you use a DNS entry for the Firebox, do not use the underscore character in the URL.

SNMP

- Fireware v10.x does not support the HA-MIB used in Fireware v9.0 or older. [23998]

General WatchGuard Server Issues

- If you already have the WatchGuard Log Server or Report Server installed and you run the WSM installer again to install the Management Server for the first time, the task bar icon for the Management Server does not appear until you reboot. [27459]
- We recommend that you do not install server software on non-English Windows 2000.
- Both the Report Server and Log Server administrative user interface email configuration require you to enable the **Server Settings tab > Send a warning if the database reaches the warning threshold** setting, at least long enough to fill in the **Send warning message to** text box. All email notifications sent from the Log and Report Servers are sent to this address. The mail sender for all email sent by Log and Report Server is set in the Notification Setup section below the Expiration Settings tab. You must enable the **Turn on notification** check box

and complete the **Send email from** text box before any email notification messages can be sent from the server.

- The Management Server, Report Server, Log Server, and Quarantine Server share the same administrative password. If you restore a back up configuration to the Management Server, the administrative password changes for all servers. [22381]
- After you change the Master Encryption Key, all WatchGuard servers must be stopped and restarted. [27416]
- Servers that are stopped will restart after the computer on which the server software is installed reboots. [2752]

Workaround

Use the Windows Services applet (Start > Programs > Administrative Tools > Services) to set the Startup Type for the appropriate service to "Manual" if you do not want the service to start automatically on when the computer starts.

Quarantine Server

- Quarantine Server does not start if the logging directory is set to a non-existent directory. [23540]

Logging / Log Server

- **Maximum Database size** setting is for threshold notification only. This setting does not limit the disk space used by the Log Server database. [27338]
- The tool to convert log files from WFS 7.x format to XML is no longer included in WSM v10.x, because it is not needed in the v10.x logging/reporting systems. The new systems can create log files and reports for Fireboxes installed with WFS appliance software.
- If you install the Log Server on a computer running Windows 2000, you must install Windows Installer 3.1 and Service Pack 4 or the Log Server does not start. [24169]

Reporting/ Report Server

- When you create a group of more than 10 Firebox devices for combined reports, the Most Popular Domain report can have incorrect byte totals. [23838]
- When your Report Server is configured to send log messages to the Log Server, and both servers are on the same computer, the Boxes Under Management report appears in the list of Report Server reports instead of in the list of Management Server reports. [23834]
- When you cancel a “load report” operation in Report Manager it can take a very long time to stop. [22887]
- The Denied Packets Summary report shows a mismatch between the reported number of records processed and the total number of attempts denied in the summary. The last device to have packets denied is not shown on the report. [23805]
- The WSM Device Manager sends a log message with the time that it inserted a device in UTC format (YYYY-MM-DDTHH:MM:SSZ). This is incorrectly presented as the local time of the Report Server. The UTC information is stripped, but the timestamp is not converted to local time. [23822]
- If you do not have your email client configured before you try to email a report from Report Manager, the email is not sent and a Java exception pops up on your screen indicating that Report Manager could not log in to the email client. [23774]
- We have made many improvements to reporting in the v10.x release. However, if you prefer to use the legacy Historical Reports tool available in previous releases of WSM, you must

continue to use your existing Log Server. The new Log Server is not compatible with previous implementations of Historical Reports. Customers, including those running appliances with WFS, who have grown accustomed to the existing report tool should thoroughly review the documentation before they upgrade to WSM v10.x.

WSM Centralized Management of Firebox X Edge devices

- The ability to configure Dead Peer Detection for Mobile User with IPSec is not available for centralized management. [29568]
- WSM cannot be used to configure the external interface of an Edge as a Wireless Client. [23081]
- The option to configure Mobile VPN with IPSec for a group is not available in WSM. [23097]
- WSM does not allow the configuration of only WAN1 or WAN2 in a multi-WAN enabled incoming policy for Edge. [23199]
- WSM does not support the configuration of 1-to-1 NAT on the Edge if the global configuration settings in WSM are enabled. [23251]
- When you configure the Mobile VPN with SSL Virtual IP address range, you must make sure that the IP address range does not overlap with those used for DHCP or PPTP. [22460]
- WSM does not change the Edge model type after you upgrade from an x10 to an x55 model in the device status tab. [15809]
- When Firebox X Edge devices are added to a centralized management configuration and changes are made that require a reboot, there is no notification that a reboot is required to apply changes. [11985]
- You cannot select WPA2 in the wireless configuration settings for Firebox X Edge e-Series devices running v8.6.x or v10.x. [21557]
- The ‘Apply to VPN’ option is not available under centralized management. There is a VPN-Any policy created for IPSec BOVPN traffic. [23195]
- Virus Outbreak Detection options appear on the Gateway AV/IPS page, but these options only apply to spamBlocker. [23180]

Management Server

- The Management Server **File > Import from File** feature does not work. To restore a Management Server configuration, use the **Backup/Restore** option available when you right-click the Management Server task bar icon. [27511]
- When a certificate for a managed Firebox is revoked, it does not show as revoked until the Management Server lease expires. [14041]
- The Management Server does not correctly recognize managed devices that use multi-WAN and have both static and dynamic external interfaces. A WSM v10.x Management Server only recognizes an Edge or Firebox X Core or Peak as static or dynamic -- but not both. BOVPN tunnels are created only to the first external interface when the Firebox has both static and dynamic external interfaces. [21416]
- A custom VPN policy template using AES encryption for phase 1 does not work with Firebox devices running Fireware v9.0 or earlier. Although the Management Server allows drag-and-drop tunnel creation between v10.x and pre v9.1 using AES for phase 1, the pre v9.1 Firebox will reject the configuration. [21627]
- If the Management Server is behind a Firebox configured in drop-in mode, and a BOPVN is created to another Firebox configured in drop-in mode, the remote Firebox cannot contact the Management Server if the BOVPN tunnel is not established. [21475]

- The default managed VPN tunnel configuration does not enable NAT-Traversal. [23756]
- When you use the default route VPN tunnel feature, all traffic from the remote networks will match the default 'ANY' policy created by the Management Server. This prevents remote BOVPN traffic from matching other firewall policies configured at the central location. To force traffic to match specific policies at the central location, VPN templates must be used. The VPN template on the Management Server must include ports that match all traffic through the BOVPN tunnel except traffic that should match firewall policies at the central location. [21965]

Firebox System Manager (FSM)

- When Firebox System Manager is connected to a Firebox for hours, there can be a small memory leak on the Firebox. [15518]
- The status of a managed BOVPN tunnel between a Firebox X Core or Peak running Fireware v10.x and a Firebox X Edge running v10.x may not show correctly in Firebox System Manager. [23413]

WatchGuard System Manager (WSM)

- After you install WSM 10.2.x the **Start Menu > All Programs** display continues to show WatchGuard System Manager 10.2.
- When you upgrade from v9.x to v10.2.x, the **Setup > Logging > Advanced Diagnostics > Set all sub-categories to same level of detail** check box is cleared. [27514]
- WSM does not show the status of a PPPoE-based WAN interface if the Firebox is configured for multi-WAN. [19564]
- The NetMeeting packet filter does not work. Use the H.323 proxy policy to allow NetMeeting traffic to pass through the Firebox. [24281]
- When your Firebox is configured in drop-in mode, the Status Report incorrectly shows the external interface subnet mask as 255.255.255.0 regardless of the actual drop-in network subnet. [21458]

Networking

- If you have a static NAT rule that uses the alias of an interface, the static NAT rule does not work if you change the interface IP address. [23502]

Workaround

Remove the static NAT rule from the policy and replace it with one that uses the IP address of the interface alias.

- When a DHCP lease renewal occurs, some unusual log messages can appear. The lease renewal succeeds and the log messages can be ignored. The log message shows as: `Deny x.x.x.x x.x.x.x icmp-Dest_Unreach code(3) 1-Trusted Firebox icmp error with data src_ip=x.x.x.x dst_ip=x.x.x.x pr=dhcp/bootp-client/udp src_port=67 dst_port=68 src_intf='1-Trusted' dst_intf='0' cannot match any flow, drop this packet 176 128 (internal policy) rc="104"` [27364]
- When you use the DHCP server with secondary networks, the DHCP server IP address given to DHCP clients is the primary interface IP address and not the secondary interface IP address. [10365]
- There is a compatibility issue between Firebox X Peak models 5000, 6000, and 8000 using Intel's CSA bus-based MAC (i82547) and the Marvell PCI bus-based MAC (88E8001). Network interfaces may sometimes negotiate at 100MB instead of 1000MB. [13659]

- Forcing the interface link speed to 1000MB, Full or Half Duplex may result in a failed interface link speed negotiation. We recommend that you always use the option to auto-negotiate link speed. [21319]
- ICMP protocol unreachable messages do not pass through the Firebox. The option to allow Protocol Unreachable messages under **Setup > Global Settings > ICMP Error Handling** does not work. [21236]

Proxies and Services

- When you use an FTP proxy policy, some active mode FTP commands can fail. FTP proxy log messages look like this when the problem occurs: `proxy[1854] 1:1193825662: ftp response '425 Can't open data connection.\x0d\x0a'` [22229]
- The default setting for the **Turn on logging for reports** option is not consistent in proxy policies. POP3 proxy traffic is logged by default, but all other proxy policies do not send log messages by default. This option controls whether proxy transaction details are shown in Traffic Monitor. [23259]
- QuickTime Video-On-Demand does not work through the HTTP proxy. [19112]
- Notification for application blocking on the TCP-UDP proxy does not work unless Intrusion Prevention is enabled for the same TCP-UDP proxy policy. [27305]
- When you enable the TCP-UDP proxy, outbound SIP connections are not correctly sent to the TCP-UDP proxy. [23546]

Workaround

Configure the SIP proxy to directly handle SIP connections.

- When you enable the TCP-UDP proxy, outbound FTP connections are not correctly sent to the TCP-UDP proxy. [23533]

Workaround

Configure the FTP proxy to directly handle FTP connections.

- The server session exit banner is made anonymous even when the **Hide Server Replies** check box is cleared in the POP3 proxy configuration. [23714]
- When you configure the SMTP proxy to strip Uuencoded and BinHex attachments, a small portion of the attachment header remains in the body of the email, together with the deny message. [22989]

Workaround

Disable stripping of Uuencoded and BinHex attachments.

- If you set the advanced logging level too high for the SMTP proxy and spamBlocker, the Firebox can become unstable when proxy traffic is at high levels. [21459]
- If a configuration contains multiple feature keys and one of the feature keys has expired, security subscriptions and signature updates fail after you upgrade to v10.x. [24050]

Workaround

Open your configuration in Policy Manager and go to **Setup > Feature Keys**. Click **Remove** one time to remove the expired feature key. Save the configuration to the Firebox.

- If you use multiple proxy policies on a Firebox X Core model X500, X700, X1000 and X2500, we recommend that you upgrade the Firebox memory to 512MB. Contact your WatchGuard reseller for information on how to purchase a 512MB memory upgrade kit.
- VoIP deployments are often complex and use many standard and proprietary protocols. Our current proxies support only standards-based traffic using H.323 and SIP protocols, for basic voice and video transfer. In VoIP industry terminology, these new proxies are more accurately called Application Layer Gateways (ALG). Some ALG features, services, and configurations may not be supported. Unsupported features include data file transfer (such as for chat, whiteboarding, fax transmission, etc), traffic control (QoS), and other limitations noted below for each protocol. Because of all these variables, we strongly recommend that you perform compatibility and interoperability tests within your own environment, before any production deployment.
- The H.323 proxy supports NAT-traversal for voice and video traffic. Note that H.323 Gatekeeper (PBX hosting/trunking) and T.120 multimedia support are not included in this release. This limits proxy use to point-to-point scenarios (such as videoconferences). While compatibility and interoperability cannot be guaranteed, point-to-point audio and video connectivity has been demonstrated with common software clients and videoconference hardware.
- Our transparent SIP proxy supports NAT-traversal for voice and video traffic. It does not provide the PBX registration capabilities of a typical standalone SIP Registrar-Proxy, but instead is an Application Layer Gateway that is transparent to SIP traffic. Although our transparent SIP proxy does support passthrough of this PBX traffic, you must have your own Registrar-Proxy server to route these connections. For this release, our transparent SIP proxy has only been tested with PBX's located on the external segment of the Firebox (hosted scenario, no trunking). While compatibility and interoperability cannot be guaranteed, point-to-point audio/video connectivity has been demonstrated with common software clients. Hosted audio connectivity has been demonstrated with various telephone handsets.

spamBlocker

- If you use both spamBlocker with Virus Outbreak Detection (VOD) enabled and Gateway AV to scan your email and the SMTP proxy detects an email message that is both spam and a virus, the SMTP proxy applies the action that is configured for VOD to the message. Specifically, if the VOD action is set to **Strip**, then the attachment(s) are removed from the message and cannot be recovered. If the VOD action is set to **Lock**, the attachment is locked in the quarantined message. [23709, 23711; all platforms]
- When spamBlocker finds a Virus Outbreak Detection (VOD) indication for an email message, all of the email's attachments are stripped or quarantined. This includes the body of the email, if the sending client has sent it in HTML format. [23485, all platforms]
- When an infected email message with multi-part attachments (i.e., embedded email messages) is detected by VOD, and Firebox is configured with the **Strip** action, a small section of the email header in the attachment remains in the delivered attachment, together with the deny message for the attachment. This header information should cause no problems because viral content is always stripped. [23550, all platforms]

- The spamBlocker Proactive Patterns feature is not available for Firebox X Core models X500, X700, X1000, and X2500. Policy Manager allows the user to configure the proactive patterns feature for non e-Series Core Fireboxes, however, the feature does not work. [21496]

Gateway AV/IPS

- The Firebox System Manager Security Services tab only updates the **Available version** information for the AV engine, AV signatures, and IPS signatures once each hour. Because of this, the displayed available version can show as older than the installed version after a manual update. You must disconnect and reconnect FSM to the Firebox to refresh the Security Services information. [21639]
- When your Gateway AV configuration is configured to lock infected email messages, an email attachment is greater than 100K bytes, and a virus is detected after the first 100K bytes, then the attachment is truncated instead of locked, even though the log message shows that the file was locked. [21489]

WebBlocker

- You must download a new full WebBlocker database for your WebBlocker Server when you upgrade from WSM 9.x or older to WSM v10.x. The WebBlocker Server database has been upgraded from 40 to 54 categories. You must do this even if you chose to keep the WebBlocker database and configuration files from the previous version of WSM. Verify your WebBlocker profile configurations after the upgrade to make sure your profile to make sure they take advantage of the new categories.
- No deny message is sent back to the client when an HTTPS connection is correctly blocked because of your WebBlocker configuration. Blocked HTTPS connections are accurately recorded in the log file. [22515, all platforms]
- If you have a v9.1 WebBlocker configuration with the **Deny All Categories** check box selected, the check box is cleared when you upgrade to WSM/Fireware v10.x. [23679]

> **Workaround**
>
> After you upgrade from v9.x or older to WSM/Fireware v10.x, you must select the **Deny All Categories** check box again and save the change to the Firebox.

User Interface

- The WSM v10.2.x software includes many bug fixes that do not affect the user interface. Any changes to the user interface included in the v10.2.x release are not localized. If you upgrade from the localized v10.1 release to the v10.2.x release, note that new UI elements remain in English. There are no updates to the localized help content.

Branch Office VPN

- If multiple IKE Phase 1 and Phase 2 proposals are configured in Policy Manager, Fireware only sends the first IKE proposal when it initiates a VPN tunnel. If Fireware does not initiate the VPN tunnel, Fireware cycles through the list of proposals until a match is found. Because of this issue it is important to have the order of the phase 1 and phase 2 proposals match on both sides of the VPN tunnel, if multiple proposals are used. [24834]
- When a certificate is revoked or renewed, a managed Branch Office VPN tunnel with a valid certificate does not appear when you start a Fireware device in drop-in mode. [11409]

Workaround

Use WSM to remove the managed Branch Office VPN tunnel and then create the tunnel again.

- Beginning with the v8.3 release, you cannot use non-ASCII characters in BOVPN shared keys. The UI does not allow you to enter non-ASCII characters in the shared key field.

Mobile VPN with IPSec

- At the end of the Add Mobile VPN with IPSec Setup Wizard, the check box to add users to the group may not be visible. [27554]

Workaround

To see the check box, expand the window size of the Setup Wizard.

- On very rare occasions, a large FTP transfer from a remote Mobile VPN client can get dropped. Specifically, this can occur if a transfer is disconnected during the phase 2 rekey. The client reconnects using the 2nd phase 2 Security Association (SA), and packets arrive from the second SA before packets from the first SA are dropped. [12340]

Workaround

Set the Phase 2 Proposal Forced Key Expiration threshold for byte count to 0 and increase the timeout setting.

Mobile VPN with PPTP

- When you configure Mobile User with PPTP, the lower half of the configuration page may not be available. [27621]

Workaround

Expand the window size to restore the full configuration page.

- When you define more than one DNS or WINS server in your network configuration, PPTP clients only get the first configured DNS and WINS server in the list. [12575]
- When the PPTP client connects to the Firebox, the connection-specific DNS suffix is not assigned [17394]

Mobile VPN with SSL

- After the Mobile VPN with SSL client first connects, any subsequent changes made to the Mobile VPN with SSL configuration will cause a connection problem with Windows Vista SP1 clients. The client appears to connect correctly, however the client sends a log message that it unsuccessfully flushed the ARP table. [29621]

Workaround

There are 2 options to work around this issue:

1. Disable User Account Control (UAC) on the Vista PC; or

2. Go to Program Files >WatchGuard >WatchGuard Mobile VPN with SSL and right-click `wgsslvpnc`. Select **Run as Administrator**.

- The Mobile VPN with SSL client may fail to connect when it is configured to have routes to 12 or more networks. The client has a limit to the number of routes it can support related to the

client configuration size. The route limit is not exact, but, depending on data in the configuration the limit is approximately 12 to 25 routes. [24226]

- The Mobile VPN with SSL client can fail to stay connected if the client computer has more then one active network interface. [27112]
- You cannot use extended ASCII characters (ä,ö,ü,ß) in a user name for Mobile VPN with SSL Active Directory authentication. [23647]
- You cannot install the Mobile VPN with SSL client on a Windows 2000 Pro computer. [22550] [23667]
- The Mobile VPN with SSL Mac client properties show only the primary WINS address, even if you have both a primary and secondary configured. [23635]

User Documentation

Documentation changes for the WSM/Fireware v10.2.7 release are included in the most current English help system available at www.watchguard.com/help/documentation. There is no updated WSM User Guide for this release.

Technical Assistance

For technical assistance, contact WatchGuard Technical Support by telephone or on the Web at http://www.watchguard.com/support. When you contact Technical Support, you must supply your registered Product Serial Number, LiveSecurity key or Partner ID.

	Phone Number
U.S. End Users	877.232.3531
International End Users	+1 206.613.0456
Authorized WatchGuard Resellers	206.521.8375